Libraries, Embedded Web Servers, and the Kitchen Sink:

Component Relationship Database (CRDb)

ICSJWG Fall 2010

CERT Vulnerability Analysis

Response

- Coordination
- Disclosure
- Mitigation

Assurance

- Discovery
- Secure configuration
- Management

Questions About Vulnerabilities

Which vendors should be notified about a vulnerability in InnerMedia DynaZip?

How does a vulnerability in GoAhead WebServer impact the Energy sector?

Which low-power wireless patient monitoring devices use the Texas Instruments MSP430 microcontroller?

Who makes the radios used in the RIM Blackberry Tour 9630?

What software should be targeted by a smart fuzzer?

Answers: Component Relationship Database (CRDb)

Collect data about the real-world, store as Resource Description Framework (RDF) models

Directed graph of hardware and software components, other necessary objects, and their interrelationships

- Vertices (nodes): hardware/software components, vulnerabilities, fixes, vendors, groups, and other objects
- Edges (lines): directional relationships
  - Node A *relates to* Node B

Answers found by tracing relationships through the graph

- RDF queries using SPARQL
- Multiple ontologies

Objects

Objects require a specific type

- Components
  - Software
  - Hardware
  - Technology (specification, standard, protocol, etc.)
- Vendor
- User
- Group
- Vulnerability
- Fix
  - Solution
  - Mitigation

Relationships

Relationships do not require a specific type

- Relationships usually have type, but CRDb (or a specific ontology) may ignore or redefine type

Relationships do require directionality

- Direction is arbitrary as long as it is defined
- Prefer a consistent direction

```
Node A : is part of : Node B
Windows XP : is made by : Microsoft
```

Other concepts

Resource Description Framework (RDF)

Web Ontology Language (OWL)

Different/multiple ontologies

Open world assumption

- Absence of information has no meaning

Strong negation

- A relationship can be made negative

```
Solaris 5 : is not made by : Microsoft
```

Resolution/specificity

- Multiple paths are possible

```
OpenSSL : uses : zlib
OpenSSL 0.9.8m : uses : zlib 1.2.4
```

Applications

Vulnerability analysis and coordination

- Identify affected components, vendors, fixes
  - More complete response
  - Improved impact assessment

Vulnerability discovery

- Better target selection, identify highly connected components

Supply chain security

- Identify sub-components, vendors

Input

Options

- Public sources
- Organizational knowledge
- Package dependencies
- Automated analysis
- Scanning
- Vendors

Considerations

- Source
- Resolution (level of detail, granularity)
- Maintenance
- Volume

Public Sources

NIST National Software Reference Library (NSRL)

Stock market

Product documentation

Acquisitions

Manual investigation

- Vulnerability analysis

Organizational Knowledge

- Camp fire stories, collective experience, investigation
- Manual process, requires UI or batch loading
- Slow
- Can be accurate

```
# Vendors that develop DNS implementations
+dns    bind bernstein_dan f5 openwall
        microsoft powerdns nominum adns
        plan9_dns inferno maradns cisco
        jhsoftware dnsmasq opendns posadis
        nlnetlabs
```

Package Dependencies

- Vendors know about dependencies
- Requires translation of package manager output

```
$ apt-cache depends openssl
  Depends: libc6
  Depends: libssl0.9.8
  Depends: zlib1g
```

- Can be automated
- Accurate

```
$ apt-cache rdepends openssl
Reverse Depends:
  slurm-llnl
  openvpn
  dovecot-common
  docbookwiki
  yaws
  xmail
  x11vnc
  ...lots more
```

Automated Analysis

Detection, similarity calculations

Source

- Text analysis

Binary

- File metadata
- Reverse engineering

```
# find . -name md5.c
./bin/md5/md5.c
./gnu/lib/libiberty/src/md5.c
./gnu/usr.bin/cvs/lib/md5.c
./lib/libc/hash/md5.c
./lib/libssl/src/crypto/md5/md5.c
./regress/sys/crypto/auth/md5.c
./sys/crypto/md5.c
./usr.sbin/bind/lib/isc/md5.c
```

```
C:\WINDOWS\system32>filever samlib.dll
--a-- W32i   DLL ENU   5.2.3790.3959 shp
47,104 02-17-2007 samlib.dll
```

Other Inputs

Scanning/fingerprinting

- VxWorks debugging service
- Banners, protocol headers
  - Shodan

Solicitation

- Ask vendors
- Ask asset owner/operators

Output

Short answer

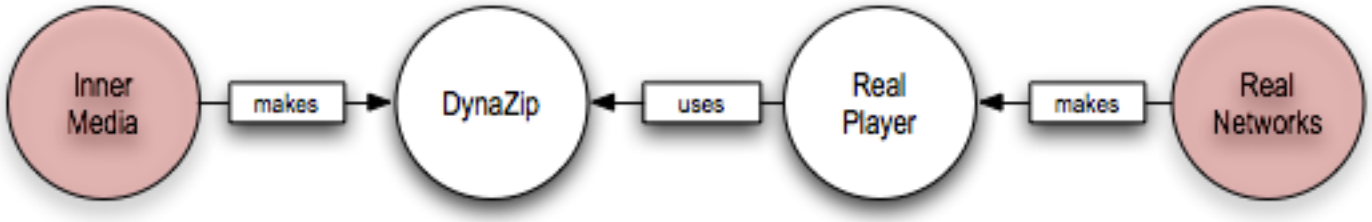
- A list of one or more objects

```
RealNetworks
```

Long answer

- Serialized graph of how the list was produced
- `InnerMedia : makes : DynaZip`
- `RealNetworks : makes : Real Player : uses : DynaZip`

Graph view



Issues

Data

- Cannot answer questions without requisite data
- Can reason about available data

Correctness

- Test “odd” real-world cases

Organization

- Do not impose one strict ontology or hierarchy

Scope

- Design supports wide range of resolution
  - Function, LOC, file name, program name, product, group
- Potential performance and data management issues

Current Test Implementation

Aduna/OpenRDF Sesame

- RDF store in PostgreSQL
- SPARQL

No ontologies yet

Data sources, management

- Python scripts
- .csv files

Sample CRDb Questions

Who is affected by WebWorks Help vulnerabilities?

Who is affected by GoAhead WebServer vulnerabilities?

VMware Help XSS

```
-----------------------------------------------------------
                VMware Security Advisory

Advisory ID:      VMSA-2009-0017
Synopsis:         VMware vCenter, ESX patch and vCenter Lab
                  Manager releases address cross-site scripting
                  issues
Issue date:       2009-12-15
Updated on:       2009-12-15 (initial release of advisory)
CVE numbers:      CVE-2009-3731
-----------------------------------------------------------

...WebWorks Help is used for creating the online help pages that
are available in VMware WebAccess, Lab Manager and Stage Manager.
```

~~VMware Help~~ WebWorks XSS

```
WebWorks.com Security Advisory 2009-0001
========================================

...

Versions Affected:
 * ePublisher 2009.2 - WebWorks Help 5.0
 * ePublisher 2009.1 - WebWorks Help 5.0
 * ePublisher 2008.4 - WebWorks Help 5.0
 * ePublisher 2008.3 - WebWorks Help 5.0
 * ePublisher 2008.2 - WebWorks Help 5.0
 * ePublisher 2008.1 - WebWorks Help 5.0
 * ePublisher 9.3 - WebWorks Help 5.0
 * ePublisher 9.2.* - WebWorks Help 5.0
 * ePublisher 9.1.* - WebWorks Help 5.0
 * ePublisher 9.0.* - WebWorks Help 5.0
 * WebWorks Publisher 8.* (includes Publisher 2003), WebWorks
   Help 4.0
 * WebWorks Publisher 7.*, WebWorks Help 3.0
 * WebWorks Publisher 6.*, WebWorks Help 2.0
```

WebWorks Users

WebWorks Customers

WebWorks solutions are used by over 2,000 corporate customers in 6,000 locations across 35 countries

WebWorks Customers include **FORTUNE 500** Companies such as:

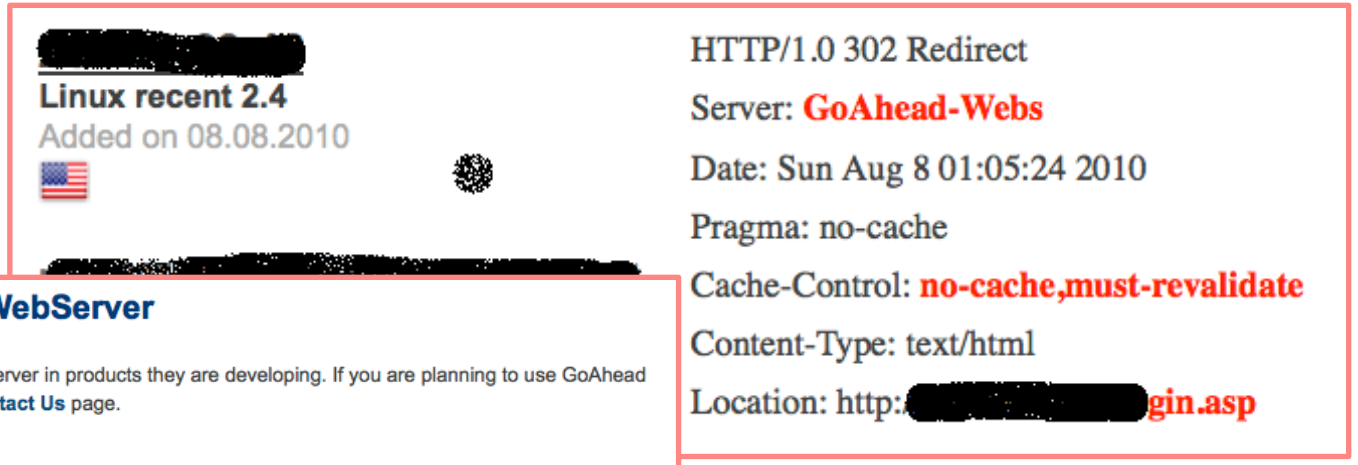
- 3M
- Agilent Technologies
- Alcoa
- Apple
- Avaya
- Boeing
- Cisco Systems
- Comcast
- Computer Sciences Corporation
- DELL
- Delta Air Line
- EDS
- EMC
- Fidelity
- Fiserv
- GE

Plus high profile companies such as...

- 20th Century Fox
- ABB
- Agfa
- Air Canada

GoAhead WebServer: Free

GoAhead WebServer: Everywhere

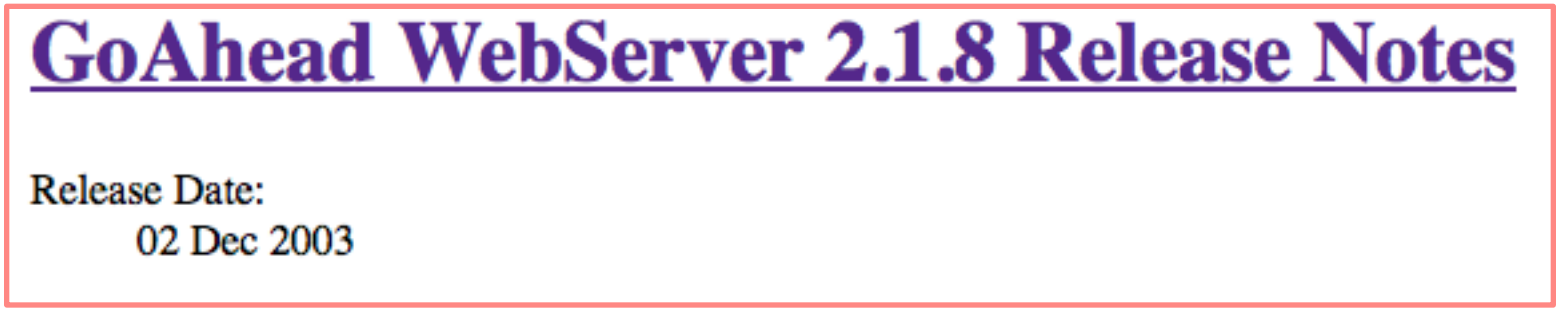


Companies using GoAhead WebServer

The following companies are using GoAhead WebServer in products they are developing. If you are planning to use GoAhead WebServer, please notify GoAhead through the **Contact Us** page.

hp invent · Honeywell · Canon · SIEMENS · SIGMET · intermec · NORTEL NETWORKS · MainStreet NETWORKS · DeTeWe · Image Research · 3Com · ci · LANCAST · RADVISION · Radiant SYSTEMS · Picasso · LARSCOM · INNO MEDIA

GoAhead WebServer: Old



GoAhead WebServer 2.1.8 Release Notes

Release Date:
02 Dec 2003

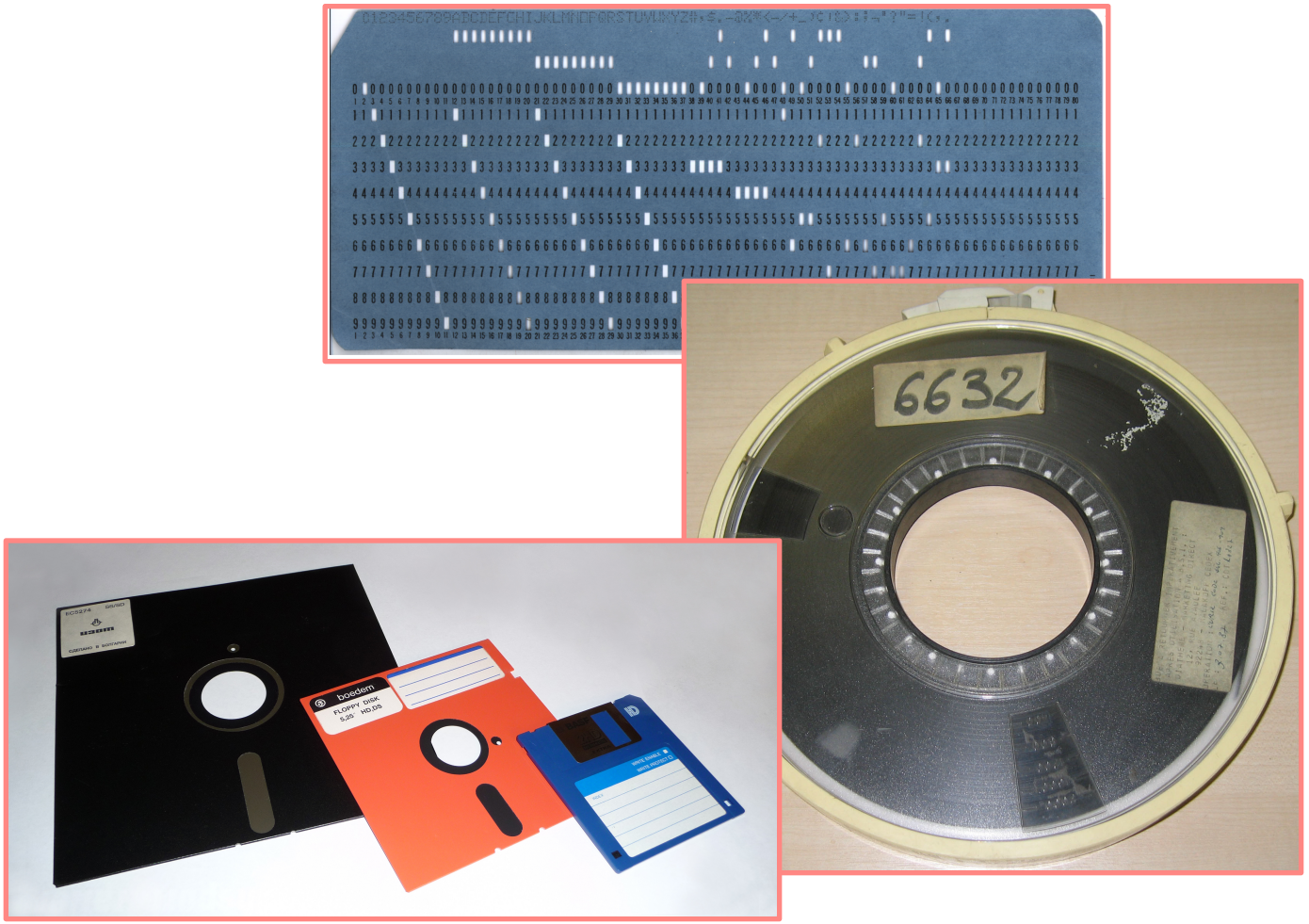
GoAhead WebServer: Vulnerable

Search Results

There are **13** CVE entries or candidates that match your search. **CVE version: 20061101**

Name	Description
CVE-2007-6702	goform/QuickStart_c0 on the GoAhead Web Server on the FS4104-AW (aka rooter) VDSL device contains a password in the typepassword field, which allows remote attackers to obtain this password by reading the HTML source, a different vulnerability than CVE-2002-1603.
CVE-2003-1569	GoAhead WebServer before 2.1.5 on Windows 95, 98, and ME allows remote attackers to cause a denial of service (daemon crash) via an HTTP request with a (1) con, (2) nul, (3) clock$, or (4) config$ device name in a path component, different vectors than CVE-2001-0385.
CVE-2003-1568	GoAhead WebServer before 2.1.6 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an invalid URL, related to the websSafeUrl function.
CVE-2002-2431	Unspecified vulnerability in GoAhead WebServer before 2.1.4 allows remote attackers to cause "incorrect behavior" via unknown "malicious code," related to incorrect use of the socketInputBuffered function by sockGen.c.

Data Call



Questions?

Art Manion

<amanioncert.org>